

Law Offices

November 20, 2015

1500 K Street N. W.  
Suite 1100  
Washington, D.C.  
20005-1209  
  
(202) 842-8800  
(202) 842-8465 fax  
www.drinkerbiddle.com

CALIFORNIA  
DELAWARE  
ILLINOIS  
NEW JERSEY  
NEW YORK  
PENNSYLVANIA  
WASHINGTON D.C.  
WISCONSIN

**By ECFS**

Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, DC 20554

RE: *Ex Parte* Submission  
*Rates for Interstate Inmate Calling Services*  
**WC Docket No. 12-375**

Dear Ms. Dortch:

Pursuant to Section 1.1206(b) of the Commission's rules, the Martha Wright Petitioners hereby submit the following information in connection with (i) the recent developments regarding the Commission's adoption of the Second Report and Order and Third Notice of Proposed Rulemaking, released November 5, 2015,<sup>1</sup> and (ii) an apparent breach of the security protocols of an ICS provider.<sup>2</sup>

**I. Securus Advice to Its Valued Customers**

The Second R&O prohibits ICS providers from marking-up mandatory taxes and regulatory fees imposed by federal, state and local governments. Moreover, the FCC specifically prohibited ICS providers from imposing discretionary or non-mandatory fees.<sup>3</sup> The clear intent of this rule was to prohibit "providers from placing a line item on a carrier's bill that implies a charge is mandated by the government when it is in fact, discretionary" in order to ensure that ICS customers are charged just, reasonable and fair ICS rates.<sup>4</sup> It is surprising, therefore, to see at least one ICS provider encourage its clients to use this language to create a new tax imposed by state or local governments.

Specifically, Securus is encouraging its valued customers to "off-set their costs related to inmate calling and investigations through the addition of a Mandatory Fee" that can be passed through by Securus to the ICS customer.<sup>5</sup> Securus takes credit that the "FCC listened to us on this matter" and promotes this new Mandatory Fee as a means to "resolve your needs for cost-recovery." Securus also indicates that it will, if necessary, utilize "change of law provisions" in their agreements to address the commission payments otherwise owed to its valued customers.<sup>6</sup>

<sup>1</sup> *Rates for Interstate Inmate Calling Services*, Second Report and Order and Third Further Notice of Proposed Rulemaking, FCC 15-136, rel. Nov. 5, 2015 ("*Second R&O*").

<sup>2</sup> *See Not So Securus – Massive Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege*, The Intercept, Nov. 11, 2015 (<http://tinyurl.com/p5qww9p>) (*See Exhibit A*).

<sup>3</sup> *Id.* ("The record in this proceeding indicates that ICS providers charge ICS end users 'fees under the guise of taxes.'").

<sup>4</sup> *Id.* (citing *Truth-In-Billing*, Second Report and Order, 20 FCC Rcd 6448, 6460-61 (2005)).

<sup>5</sup> *See Letter to Valued Customer*, Securus Technologies ("*Securus Letter*") (*See Exhibit B*).

<sup>6</sup> *Securus Letter*, pg. 2.

It is also surprising, but very encouraging, that Securus no longer believes that the implementation of the *Second R&O* will be a “business-ending event”<sup>7</sup> or will result in the elimination of service from any location. Instead, Securus assured its customers that:

If the Order does become effective, we do not plan to eliminate service from any location or significantly reduce any service levels due to implementation. You have our promise on this.<sup>8</sup>

In sum, in response to the adoption of the *Second R&O*, Securus will (i) invoke change of law provisions to eliminate commission payments, (ii) encourage its valued customers to impose new taxes on ICS customers as a result of its refusal to pay commissions moving forward, but (iii) promise not to eliminate service from any location, presumably because it will cease paying commissions.

## **II. Securus Security Breach**

Just as alarming as Securus’ campaign for the creation of new government taxes on ICS is the recent news that 70 million telephone calls between inmates and their families, loved ones and attorneys were released as a result of a hack or breach of security. As noted in the attached *The Intercept* article, included in this breach was information relating to approximately 14,000 attorney/client phones calls which were recorded by Securus.<sup>9</sup>

While Securus believes that these conversations were recorded with prior consent,<sup>10</sup> it is unclear whether the information obtained through the hack/breach contained information that would be considered Customer Proprietary Network Information (“CPNI”) as defined by Section 222 of the Communications Act of 1934, as amended. ICS providers are subject to the Commission’s CPNI regulations, and file annual statements regarding their compliance with the Commission’s rules.<sup>11</sup>

This is a valid concern because recent technological developments by ICS providers such as Securus and Global Tel\*Link<sup>12</sup> have begun to track the location of wireless customers that receive calls from inmates. For example, Securus touts its “Location Based Services” which involves:

---

<sup>7</sup> *Prison Phone Company Fights To Keep Profiting Off Inmates and Their Families*, Oct. 21, 2015 (<http://tinyurl.com/pw5wtqj>) (See Exhibit C).

<sup>8</sup> *Securus Letter*, pg. 2.

<sup>9</sup> Securus’ recently acquired subsidiary, JPay, Inc., follows the same approach. See *No Bar to Profit – Prison Contractor Pushes Pricey Tech Services* (<http://tinyurl.com/naukpol>) (“JPAY...records all conversations and has no system in place to weed out privileged attorney calls...It’s a system built for visitors, for family members and friends...It’s not built for the attorney part of it.”).

<sup>10</sup> See *Securus Provides Updates on Investigation into Stolen Data Records*, Nov. 13, 2015 (<http://tinyurl.com/pflgw57>) (See Exhibit D).

<sup>11</sup> See 47 C.F.R. §64.2009(e)(2015) (See also Exhibit E).

<sup>12</sup> GTL’s product is called LocationIQ™, and Telmate’s product is called Investigator. (See Exhibit F).

collecting the approximate location of a cellular telephone, through the cellular provider, as soon as the called party accepts the call from the inmate. The originating location as well as the location of the cellular telephone at the end of the call is recorded and available for research and investigation. LBS is not dependent on cellular telephone GPS settings, which can be turned off by users seeking to escape tracking. This is a great advantage, ensuring that your facility knows where your inmates are calling even when the billing name and address of the called party might not be known.<sup>13</sup>

These services provide “real-time alerts” tracking the proximity of wireless callers’ to correctional facilities, or flagging those located “in an area of interest.” *Id.* If location-based information relating to ICS customers is being collected by ICS providers, it may be necessary to determine if proper consent was obtained from the recipients.

The Commission has recognized that “location information in particular can be very sensitive customer information.”<sup>14</sup> Under Section 222(f) of the Communications Act, “without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to call location information concerning the user of a commercial mobile service . . . or the user of an IP-enabled voice service.”<sup>15</sup>

According to the Commission, “Section 222(f)’s requirement of ‘express prior authorization’ leaves no doubt that a customer must explicitly articulate approval before a carrier can use that customer’s location information.”<sup>16</sup> In addition, “Section 222(f)’s requirement of ‘express prior authorization’ . . . cannot be satisfied by a customer’s silence in response to a carrier’s notice of intent to use location information.”<sup>17</sup>

When implementing other privacy provisions into its rules, the Commission concluded that “Express Prior Authorization may be obtained by oral or written means, including electronic methods,”<sup>18</sup> but such authorization must be carefully documented. “Written authorization must contain the subscriber’s signature, including an electronic signature,”<sup>19</sup> while carriers “who choose to obtain authorization in oral format are also expected to take reasonable steps to ensure that such authorization can be verified.”<sup>20</sup>

---

<sup>13</sup> See *Securus Location Based Services* (<http://tinyurl.com/nbbulpx>) (See Exhibit G).

<sup>14</sup> *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, nt. 54 (2013).

<sup>15</sup> 47 U.S.C. § 222(f) (2015).

<sup>16</sup> *In the Matter of Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices*, Order, 17 FCC Rcd 14,832, ¶ 5 (2002).

<sup>17</sup> *Id.* at nt. 16.

<sup>18</sup> 47 C.F.R. § 64.3100(d) (2015).

<sup>19</sup> *Id.* at § 64.3100(d)(1).

<sup>20</sup> *In the Matter of Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, Order, 19 FCC Rcd 15,927, ¶ 43 (2004). See also 47 C.F.R. § 64.2007(a)(2015).

Thus, it is unclear whether ICS providers that track the location of their wireless customers have received proper authorization. Even if wireless ICS customers did grant express prior authorization, the fact remains that this information may be leaked or hacked as discussed in *The Intercept* article.

However, even if the hack/breach did not occur, the question of whether express prior authorization has been granted by ICS consumers for the sale of their CPNI must be addressed. In particular, Securus apparently makes available customer CPNI information to parties that sign up for its Threads™ service. According to Securus, customers that sign up for this service obtain access to:

- More than 600,000 people with billing name and address (not incarcerated)
- More than 950,000 inmates
- More than 1,900 correctional facilities
- More than 100,000,000 call records between inmates and called parties<sup>21</sup>

Additionally, the Threads™ provides the following information:

- Calling patterns
- Linkage analysis
- Inner circle identification (suspects' inner working group)
- Bounce list hit notifications (is the inmate calling someone on your staff?)
- Associations
- Chain dialing
- Interactive maps
- The most likely leader of a criminal organization

The Threads™ Use Agreement and Community Use Agreement are attached hereto as Exhibit H. While the agreements require the Threads™ customer to ensure it complies with all privacy laws, it is not clear that the original collection of this information by Securus complies with the FCC's CPNI requirements.

In light of the vast collection of CPNI, which is apparently available to paying subscribers, and in light of the apparent hack/breach of 70 million phone calls which apparently contained information covered under the Commission's CPNI rules, the Commission should seek additional information into whether this breach raises CPNI or other consumer privacy concerns. A recent decision involving the theft of customer information from a cable company may represent an appropriate approach for the Commission to review this matter.<sup>22</sup>

---

<sup>21</sup> See Securus Threads™ (<http://tinyurl.com/nmxr7jn>) (See Exhibit H).

<sup>22</sup> See *Cox Communications to Pay \$595,000 to Settle Data Breach Investigation*, Order and Consent Decree, DA 15-1241 (Nov. 5, 2015).

Should you have any questions regarding these matters, please contact undersigned counsel.

Respectfully submitted,



Lee G. Petro

*Counsel for Martha Wright Petitioners*

cc (by/email):

Chairman Thomas Wheeler  
Commissioner Mignon Clyburn  
Commissioner Jessica Rosenworcel  
Commissioner Ajit Pai  
Commissioner Michael O'Rielly  
Jonathan Sallet, General Counsel  
Travis LeBlanc, Chief, Enforcement Bureau  
Matt DelNero, Chief, Wireline Competition Bureau  
Gigi Sohn, Counselor to Chairman Wheeler  
Rebekah Goodheart, Legal Advisor to Commissioner Clyburn  
Travis Litman, Legal Advisor to Commissioner Rosenworcel  
Nicholas Degani, Legal Advisor to Commissioner Pai  
Amy Bender, Legal Advisor to Commissioner O'Rielly  
Pamela Arluk, Chief, Pricing Policy Division, Wireline Competition Bureau  
Lynne Engledow, Acting Deputy Chief, Pricing Policy Division, Wireline Competition Bureau

**EXHIBIT A**

# Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege

Nov. 11, 2015 16 min read [original](#)

AN ENORMOUS CACHE of phone records obtained by *The Intercept* reveals a major breach of security at Securus Technologies, a leading provider of phone services inside the nation's prisons and jails. The materials — leaked via [SecureDrop](#) by an anonymous hacker who believes that Securus is violating the constitutional rights of inmates — comprise over 70 million records of phone calls, placed by prisoners to at least 37 states, in addition to links to downloadable recordings of the calls. The calls span a nearly two-and-a-half year period, beginning in December 2011 and ending in the spring of 2014.

Particularly notable within the vast trove of phone records are what appear to be at least 14,000 recorded conversations between inmates and attorneys, a strong indication that at least some of the recordings are likely confidential and privileged legal communications — calls that never should have been recorded in the first place. The recording of legally protected attorney-client communications — and the storage of those recordings — potentially offends constitutional protections, including the right to effective assistance of counsel and of access to the courts.

“This may be the most massive breach of the attorney-client privilege in modern U.S. history, and that’s certainly something to be concerned about,” said David Fathi, director of the ACLU’s National Prison Project. “A lot of prisoner rights are limited because of their conviction and incarceration, but their protection by the attorney-client privilege is not.”

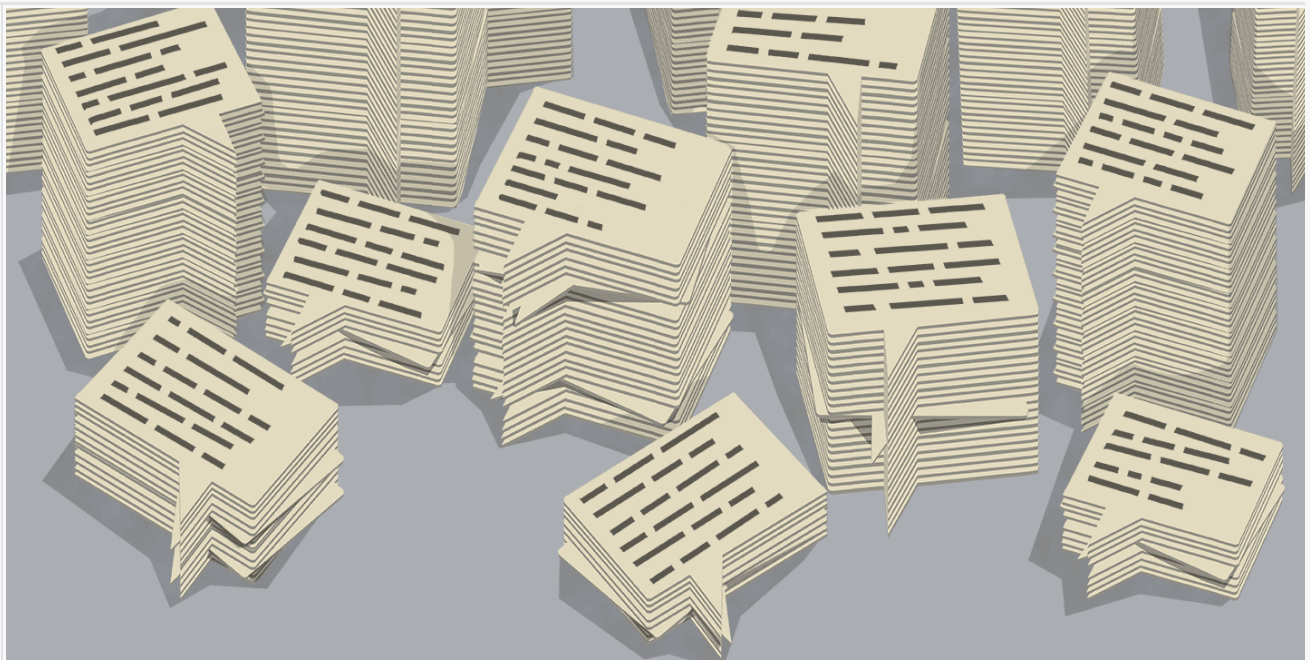
The blanket recording of detainee phone calls is a fairly recent phenomenon, the official purpose of which is to protect individuals both inside and outside the nation’s prisons and jails. The Securus hack offers a rare look at this little-considered form of mass surveillance of people behind bars — and of their loved ones on the outside — raising questions about its scope and practicality, as well as its dangers.

Securus markets itself to government clients as able to provide a superior phone system — its Secure Call Platform — that allows for broad monitoring and recording of calls. The company also promotes its ability to securely store those recordings, making them accessible only to

authorized users within the criminal justice system. Thus, part of the Securus promise is not only that its database is vast, but also that it meets rigorous standards for security. “We will provide the most technologically advanced audio and video communications platform to allow calls with a high level of security,” reads the company’s Integrity Pledge. “We understand that confidentiality of calls is critical, and we will follow all Federal, State, and Local laws in the conduct of our business.”

But the fact that a hacker was able to obtain access to over 70 million prisoner phone call records shows that Securus’ data storage system is far more vulnerable than it purports to be.

More broadly, the Securus leak reveals just how much personal information the company retains about prisoners and the countless people to whom they are connected. It is information that, in the narrow context of incarceration, may not be considered private, but in the larger world raises serious questions about the extent to which people lose their civil liberties when their lives intersect, however briefly, with the criminal justice system.



*Illustration: Alexander Glandien*

SECURUS IS A TELECOMMUNICATIONS company based in Dallas, Texas, owned by a private equity firm. Its primary business is providing phone and video visitation services to incarcerated people — ostensibly offering a meaningful way for them to keep in touch with loved ones on the outside, as well as to communicate with attorneys. Until now, Securus was probably best-known for the incredibly high rates it has traditionally charged for phone calls, a burden borne almost exclusively by the very people who are the least able to afford it. (The Federal Communications Commission in October voted to cap calling rates and fees, a move

that Securus and other industry leaders had fought, claiming the change would have a “devastating effect” on their businesses.)

It isn't just Securus whose business model has relied on gouging people caught up in the criminal justice system. The industry's other players, including the leading prison telecom company, Global Tel\*Link, largely do the same. Prison and jail communications is a \$1.2 billion a year business, whose handsome profits come from serving a captive and inelastic market. According to public relations materials, Securus provides communications platforms used by more than 1.2 million inmates across the country, who are confined in more than 2,200 facilities; by 2012 the company was processing more than 1 million calls each day. In 2014, Securus took in more than \$404 million in revenue.

Securus does business with local and county governments (which operate the nation's jails) and with state departments of correction (which, with some exceptions, run the nation's prison systems). A key selling point to its clients is that the company not only installs and maintains phone systems at little to no cost to the government, but also that it agrees to pay back to its clients generous “site commissions,” a kickback that comes from revenue generated by inmate calls — on average 42 percent of the revenue from its state contracts, according to [research](#) done by *Prison Legal News*. (The FCC rate caps threaten the industry's ability to keep revenues large enough to fund the exorbitant kickback scheme it created. Lowering and capping the rates and fees charged for calls means at least some industry players could be forced to dip into company coffers in order to comply with contracted payoff schedules, unless they renegotiate existing contracts. How the new rate caps will impact these payoffs remains to be seen.)

“OMG ... this is not good!” reads an internal Securus email discussing phone calls hacked in 2014.

In addition to the sweetheart deal it offers clients, Securus also touts the technology of its Secure Call Platform, which allows recording and monitoring, with few exceptions, of all calls made by prisoners. The superior technology, it claims, ensures that its database is well-protected, and only accessible to authorized users — among them corrections workers, police investigators, and prosecutors. Law enforcement personnel are particularly important to the company: Securus promises it can provide recordings on demand to investigators across jurisdictions, promoting its system as a powerful crime-solving tool.

But the scale of the Securus hack shows the company has failed to fulfill its own promises on security. The more than 70 million phone call records given to *The Intercept* include phone calls placed to nearly 1.3 million unique phone numbers by more than 63,000 inmates. The original data was contained in a 37-gigabyte file and scattered across hundreds of tables, similar to

spreadsheets, which *The Intercept* merged into a single table containing 144 million records. A search for duplicates reduced this figure to more than 70 million records of individual phone calls.

The database contained prisoners' first and last names; the phone numbers they called; the date, time, and duration of the calls; the inmates' Securus account numbers; as well as other information. In addition to metadata, each phone call record includes a "recording URL" where the audio recordings of the calls can be downloaded.

The vast majority of the calls appear to be personal in nature; downloaded audio files leaked alongside the larger database of recordings include one in which a couple has an intimate conversation; in another, relatives discuss someone whose diabetes is worsening. In a third, a couple discusses *Dancing With the Stars*, TV dinners, and how much money is available to pay for their regular phone conversations — versus how much should instead be spent on food. But a subset of the recordings — a minimum of roughly 14,000 — were made by detainees to attorneys, in calls that range from under a minute to over an hour in length.

To arrive at this figure, *The Intercept* looked up each of the nearly 1.3 million phone numbers that inmates called in a public directory of businesses to find out whether a law firm or attorney's office is associated with that number. We found that Securus recorded more than 14,000 phone calls to at least 800 numbers that clearly belonged to attorneys. That 14,000 figure, however, is likely an underestimate because it does not include calls to attorney cellphone numbers. In other words, the 14,000 attorney calls are potentially just a small subset of the attorney-client calls that were hacked.

In short, it turns out that Securus isn't so secure.

In fact, this doesn't seem to be the first time that Securus' supposedly impenetrable system has been hacked. According to documents provided to *The Intercept* by a Texas attorney, the company's system was apparently breached just last year, on July 18, 2014, when someone hacked three calls made by an inmate named Aaron Hernandez, presumably the former player for the New England Patriots, who was awaiting trial for killing a friend. In an email thread from July 21, 2014, two Securus employees discuss the breach — the system was accessed by someone in South Dakota, they discover, though they don't have that person's name. "OMG.....this is not good!" reads one email contained in the document. "The company will be called to task for this if someone got in there that shouldn't have been."

There is no indication the 2014 hack has previously been made public. Securus did not respond to numerous requests for comment for this story. [Editor's note: See update below for a statement

*from Securus in response to publication of this story.]*

PRISONERS DO NOT GENERALLY ENJOY a right to privacy while incarcerated — a fact that is emphasized in the course of virtually any communication with the outside world. Like other jail and prison telecoms, Securus inserts a recorded message at the beginning of each prisoner-initiated phone call, reminding recipients that “this call is from a correctional facility and may be monitored and recorded.” In this context, anyone who hears the warning and still chooses to use the phone has effectively waived a right to privacy during that call, a condition all too familiar to people with incarcerated loved ones. Still, it is hard to imagine that people on either end of the line would ever anticipate that their conversations would be stored for years, in a manner that could potentially expose their intimacies to the larger public. By failing to prevent hackers from accessing the calls, Securus appears to have done just that.

This is troubling to the ACLU’s Fathi, because “waivers of rights are not meant to be all or nothing. Waivers are meant to be only as extensive as necessary to accomplish the goal underlying the waiver,” he said. If the goal for recording and monitoring detainee phone conversations is to enhance safety both inside and outside a facility that’s one thing — but those conversations should not be stored indefinitely, once they’re determined to be free of intelligence that would aid the institutional goal.

The mass recording of detainee calls was originally rationalized as improving safety within a facility — a way to hedge against contraband being brought in, to ferret out escape attempts or potentially violent uprisings, and to curb the possibility of witness tampering or intimidation. But if the goal is to see if a “person is smuggling drugs [or] plotting an escape,” said Fathi, “it doesn’t mean that the prisoner and the ... outside person they’re talking to has forever waived all privacy rights and that any conceivable use of that recording is OK.”

The implications are especially alarming for calls that are understood to be the exception to the record-everything rule. Securus’ phone systems are supposed to be set up to allow certain phone numbers to be logged and flagged so that calls to those numbers are exempt from being recorded — let alone stored.

Indeed, that a criminal defendant or inmate should be able to speak frankly and honestly with a lawyer is a cornerstone of the criminal justice system — inherent in a defense attorney’s ethical obligations, and firmly rooted in the Sixth Amendment right to competent and effective legal counsel. A review of contracts and proposals completed by Securus in a handful of states reflects the company’s understanding of this right. In a 2011 bid to provide phone service to inmates in Missouri’s state prisons, Securus promised that each “call will be recorded and monitored, with the exception of privileged calls.” But the database provided to *The Intercept*

shows that over 12,000 recordings of inmate-attorney communications, placed to attorneys in Missouri, were collected, stored, and ultimately hacked.



*Illustration: Alexander Glandien*

The data provided to *The Intercept* also includes at least 27 recordings of calls to attorneys in Austin, Texas, made between December 2011 and October 2013 — a fact that is particularly compelling in light of a federal civil rights suit filed there in 2014 against Securus, which provides phone service to the county's jails. At the heart of the lawsuit is the allegation that calls to known attorneys have been — and continue to be — recorded. The company's contract specifically provides that calls "to telephone numbers known to belong [to] attorneys are NOT recorded" and that "if any call to an attorney is inadvertently recorded, the recording is destroyed as soon as it is discovered."

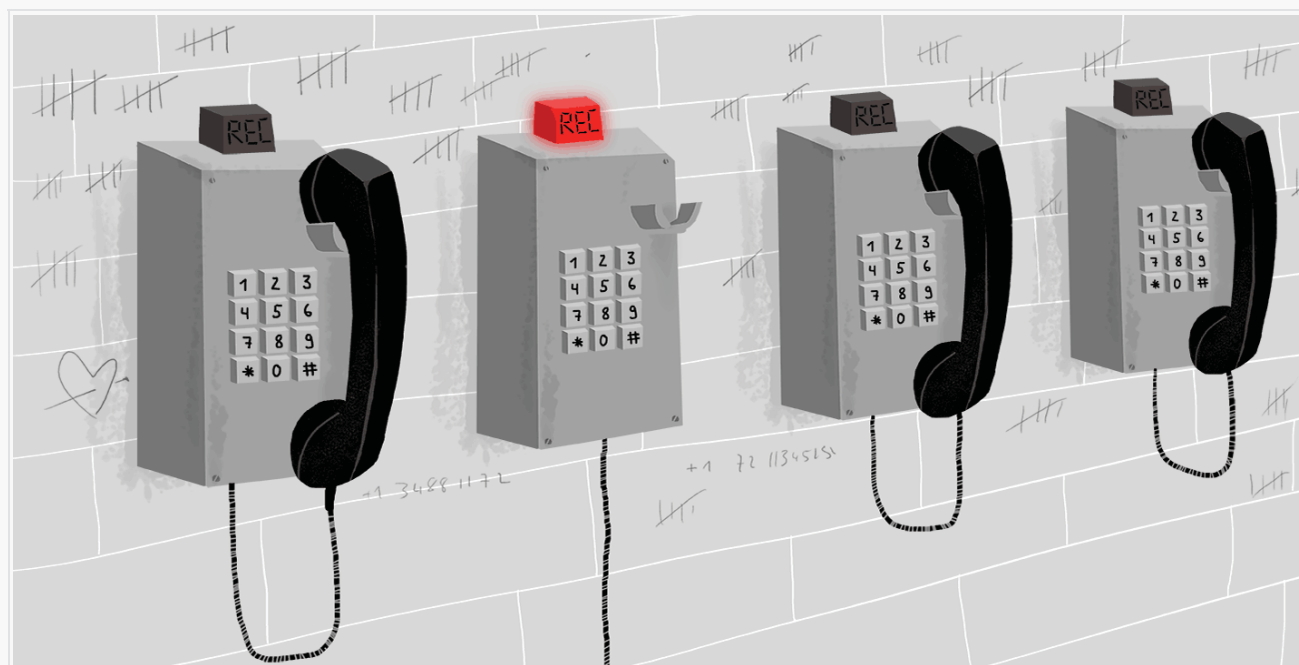
The lawsuit was brought by the Austin Lawyers Guild, four named attorneys, and a prisoner advocacy group, and alleges that, despite official assurances to the contrary, privileged communications between lawyers and clients housed in the county jails have been taped, stored, "procured," and listened to by prosecutors. The plaintiffs say that while some prosecutors have disclosed copies of recordings to defense attorneys as part of the regular evidential discovery process, other prosecutors have not, choosing instead to use their knowledge of what is in individual recordings to their "tactical advantage" in the courtroom "without admitting they obtained or listened to the recordings." (None of the recordings provided to *The Intercept* appear to be connected to any of the Austin attorneys named in the suit.)

The Austin attorneys argue that the intrusion into their communications with clients

undermines their ability to effectively represent them. And those most disproportionately impacted are often clients who are the most disadvantaged: those who can't afford bail and have to stay in jail awaiting prosecution. Austin defense attorney Scott Smith, who discovered this summer that an intern in the prosecutor's office had inadvertently listened to a portion of a phone call he had with a jailed client, points out that it rigs the adversarial legal process in favor of the state. "How do you plan your strategy? It's like being at the Superbowl and one team gets to put a microphone in the huddle of another team."

Challenging the lawsuit, Securus notes that government intrusion into the attorney-client relationship could be a violation of the Sixth Amendment. But the company insists it has abided by its policy of not recording privileged phone calls — while at the same time maintaining that any existing tapes were voluntarily turned over by the state to defense attorneys during discovery. What's more, Securus argues that the plaintiffs have not proved that "such recordings" had any adverse effects on their cases. "Securus acknowledges that Plaintiffs have alleged that recorded attorney-client calls have been shared with prosecutors, but they have failed to articulate a single instance where they have been harmed or prejudiced," Securus said.

Exactly who is to blame for the recording of attorney calls is unclear. In many jurisdictions — including in Austin — the onus is on lawyers or their clients to give phone numbers to prison officials so that they can be placed on a do-not-record list. Failing to provide up-to-date contact information would make any inadvertent recordings the attorney's or inmate's fault. But properly logging these numbers is the government's responsibility. And the secure storage of these is squarely up to Securus — particularly given that it markets itself as providing a service to do exactly that.



*Illustration: Alexander Glandien*

IT WASN'T ALWAYS THE CASE that detainee phone calls were recorded in bulk. The practice really took hold in the 1990s, says Martin Horn, a lecturer at John Jay College of Criminal Justice in New York, who previously served as commissioner of the New York City Department of Correction and, before that, as secretary of corrections in Pennsylvania. When Horn went to Pennsylvania in 1995, the state did not allow for the recording of inmate calls. But that decade saw “numerous horror stories,” he said, of inmates “perpetrating crimes” from within prison, “continuing to run their criminal enterprises” from behind bars, or “threatening witnesses, and so on.” At the same time, telephone technology had evolved significantly, making monitoring, recording, and storage of call data possible.

Until the mid-1980s, inmate phone services were provided by AT&T via operator-assisted collect calls from pay phones. But after the breakup of AT&T the market became more competitive — and less regulated — and companies such as Securus, originally known as the Tele-Matic Corporation, entered the market to offer equipment and, ultimately, sophisticated monitoring systems.

Today, Horn regards call monitoring as an important correctional tool. And while Horn said he was never made aware of any recording of attorney-client communications during his time in corrections, he said to the extent that a privileged communication is either monitored or recorded, there isn't necessarily a harm — “if in the course of listening to it you become aware that it's a conversation with a privileged party, such as an attorney, you stop listening,” he said. “So the fact that it was recorded, while unfortunate, you know, isn't necessarily damaging.”

The hacked database also includes records of calls between prisoners and prosecutors — including 75 calls to a U.S. attorney's office in Missouri.

But the massive amount of data provided to *The Intercept* suggests that the scope of surveillance within the system goes far beyond what the original goals might have been. A 2012 Securus contract with the Illinois Department of Corrections describes an optional product called Threads, branding it “one of the most powerful tools in the intelligence community.”

“Securus has the most widely used platform in the industry, with approximately 1,700 facilities installed, over 850,000 inmates served, literally petabytes of intelligence data, and over 1 million calls processed per day,” the company bragged to Illinois officials. “This valuable data is integrated directly into Threads and could be available at [Department of Correction]'s and [Department of Juvenile Justice]'s fingertips.”

Today those numbers are even higher. Securus' website says that the Threads database contains the billing names and addresses of over half a million people who are not incarcerated, as well as information about more than 950,000 inmates from over 1,900 correctional facilities, and includes over 100 million call records. The amount of data sold to corrections and law enforcement investigators "continues to grow every day."

As Adina Schwartz, a professor at John Jay College, points out, when you consider that these recordings can be stored "forever, with no supervision," the potential for abuse increases. "I think any criminal defense attorney who wasn't worried by that prospect is basically somebody who doesn't do his or her job."

And the recordings with known attorneys are not limited to calls with defense lawyers. The hacked database also includes records of calls between prisoners and prosecutors — including 75 calls to a United States attorney's office in Missouri. These, too, are potentially problematic, particularly if they include conversations with cooperating witnesses who could be vulnerable if the details of their dealings with the government were exposed.

The attorney-client privilege is "the oldest privilege of confidentiality known in our legal system," said Fathi. In a criminal case it prohibits defense attorneys from divulging, or prosecutors from using, any case-related information that was obtained in confidence. But the reality is that keeping conversations with incarcerated defendants confidential is a challenge. Experts point out that the recorded notice embedded within phone calls initiated inside jails and prisons means that there should be no real expectation of privacy. "If a client is making an out-of-prison call to an attorney, the attorney-client privilege, arguably, doesn't apply," said Michael Cassidy, a professor of law at Boston College Law School, because by consenting to speak over a phone line that is subject to recording, the client and attorney should expect that is happening. But that isn't the end of it: Even if the privilege doesn't apply, "the Sixth Amendment right to counsel applies and the government can't interfere with it," he said. "So even if you could argue that notifying a prisoner that their calls are being recorded negates the privilege, it doesn't negate the Sixth Amendment right to not have the government interfere with counsel." And monitoring, recording, and potentially using information gleaned from attorney-client calls would do just that.

That's why prison calling systems, such as Securus' Secure Call Platform, are set up to log numbers that should not be recorded. "But that's a technological issue and sometimes it doesn't work," said Cassidy.

But Schwartz argues that the logging of attorney phone numbers provides a "recognition that there is attorney-client privilege" and that it is "incumbent on the government to follow

through” in protecting that privilege. When attorneys learn that their calls have been recorded, it shakes the foundation of trust, inevitably impinging on their Sixth Amendment obligations. “Once people know there is trickery, there is a chilling of attorney-client communications — because how do you know it won’t happen again?” Schwartz asked.

Indeed, that is precisely the risk that Fathi sees arising from the breach of Securus’ database. “Going forward, prisoners will have very good cause to question whether their phone calls with their attorneys are confidential. And that undermines that very core and fundamental purpose of the attorney-client privilege, which is to allow persons consulting an attorney to give a full and frank account of their legal problem,” he said.

Still, challenging the recording could be tricky, says Cassidy, even if there is clear evidence of taped communications. If a call was recorded because the attorney or client failed to put a phone number on the do-not-record list, he says, then the state is off the hook — a prisoner can’t sue for damages, or seek to have his or her criminal charges dismissed (although the government would still be prohibited from listening to or using the content of the call). However, if one can “show a regular and systemic practice” of recording such calls, a case could be made that “the company is violating multiple prisoners’ Sixth Amendment rights,” which could have more of an impact, perhaps prompting systemwide reforms.

And Fathi believes a case could also be made that the recording and storing of non-attorney calls is unconstitutional. “Prisoners do retain some privacy rights and certainly people on the outside who just happen to be talking to prisoners retain privacy rights. And, again, the fact that you’re passively consenting that the call can be monitored for security purposes doesn’t mean you’re consenting to all conceivable uses of that recording for all time,” he said. “I think even with the non-attorney calls there may be a case to be made that this is just so spectacularly overbroad that it is unconstitutional.”

Indeed, Austin attorney Scott Smith believes that, at least in the nation’s jails — where the majority of inmates are awaiting prosecution and have not yet been found guilty of anything — the blanket recording of phone calls should be stopped. If there are specific detainees worth monitoring, that can be accomplished in a far less intrusive manner, he said. “You can say safety mandates a reduction of civil liberties all the time. And that’s essentially the old debate — how much do you have civil liberties and how much do you need to get rid of them in order to be safe?”

Fathi agrees that the practice of recording detainee phone conversations should be reined in and limited. “It is another manifestation of the exponential growth of the surveillance state.

Obviously that's been noticed and commented upon in other contexts, but if we're talking about [more than 70] million [calls], even if some of those are repeat calls between the same people, that's a lot of people — including non-prisoners whose privacy has been compromised by a private company that is acting as an agent of the government," he said.

### **Update: November 12, 2015**

After this story was published, Securus emailed the following statement:

Securus is contacting law enforcement agencies in the investigation into media reports that inmate call records were leaked online. Although this investigation is ongoing, we have seen no evidence that records were shared as a result of a technology breach or hack into our systems. Instead, at this preliminary stage, evidence suggests that an individual or individuals with authorized access to a limited set of records may have used that access to inappropriately share those records.

We will fully support law enforcement in prosecution of any individuals found to have illegally shared information in this case. Data security is critically important to the law enforcement and criminal justice organizations that we serve, and we implement extensive measures to help ensure that all data is protected from both digital and physical breaches.

It is very important to note that we have found absolutely no evidence of attorney-client calls that were recorded without the knowledge and consent of those parties. Our calling systems include multiple safeguards to prevent this from occurring. Attorneys are able to register their numbers to exempt them from the recording that is standard for other inmate calls. Those attorneys who did not register their numbers would also hear a warning about recording prior to the beginning of each call, requiring active acceptance.

We are coordinating with law enforcement and we will provide updates as this investigation progresses.

*Research: Margot Williams, Joshua Thayer*

**EXHIBIT B**

November 13, 2015



Subject: FCC Order on Inmate Calling Rates and Impact on Industry and Correctional Facilities

Dear Valued Customer:

On October 22, 2015, the Federal Communications Commission (FCC) in a 3-2 vote approved an Order that will drastically impact inmate telephone end-user rates, site commissions, carrier reporting requirements, future technology development, and ancillary services and fees. The purpose of this letter is to alert you to this issue and provide you with information on how this Order impacts you.

Late last week, we received an advanced copy of the inmate calling rate Order. This still must be published in the Federal Register to become effective; however, we do believe this represents the final wording on this Order.

#### **Overview of the Order**

The written Order is 210 pages long and is full of errors in fact, analysis, and conclusion.

The Order sets weighted average (when considering the distribution of inmates across facilities) rate caps of \$.1188 per minute by using the cost study submissions of all inmate telephone providers. Securus used a highly regarded third party consulting firm to review and submit Securus' costs to the FCC. This firm calculated our costs at \$.1776 per minute—49% higher than the weighted average rate cap of the industry. Effectively, this means that the FCC ignores the differences between platforms, technology, and capabilities in competitors, and under values high technology providers, such as Securus.

Site commissions are a focal point of the Order. The word "commissions" appears 209 times in the written Order. The FCC puts a primary blame on site commissions for high inmate rates. To drive out commissions, the FCC instructed inmate telephone providers to submit their costs without including commissions, then the FCC used this data and set rate caps below these costs to insure commissions are effectively eliminated. Further, to make sure that even low cost/low technology providers can't continue to pass commissions through to end-users, the Order requires all providers to annually certify and report on any commissions paid and states the FCC will use this as evidence to systematically continue lowering rate caps until providers cease paying commissions.

The attached Fact Sheet provides you with more information on important details of the Order.

#### **Securus Perspective**

As stated above, the Order is full of errors in fact, analysis, and conclusion. Setting rate caps below costs, impacting existing contracts, and failing to understand the value of protecting future technological advancements, are very important issues concerning us. We are carefully studying our appeal options at this point.

However, it appears that the FCC did listen to us regarding the importance of continued funding of correctional facilities and included in the Order the ability for you to get a Mandatory Fee authorized and assessed, over and above the rate cap, that can be passed on to consumers. Essentially, the FCC is requiring inmate telephone providers to price services within rate caps, but, allows government bodies to off-set their costs related to inmate calling and investigations through the addition of a Mandatory Fee. This addition to the Order provides important relief to you and is an approved and legal way for you to continue to generate some level of funding through inmate calling services. We are pleased about this addition and that the FCC listened to us on this matter.

We believe that the Mandatory Fee provision in the Order can help resolve your needs for cost-recovery. Our attention now shifts to finding ways to reduce our costs and continue to create advances in technology development within the constraints of this Order.

We recognize there is a lot of industry and market confusion on the status of site commissions with this Order. A few companies say that because the FCC did not actually prohibit the payment of site commissions, they are still eligible to be paid, albeit at lower levels than before. From our perspective, these companies are either trying to interfere and disrupt change of law negotiations between competitors and their customers for the purpose of creating bad-will between the parties; or, in the case of continuing to pay smaller amounts of commissions to their own customers, they are creating a situation where the FCC can come back again and again and further reduce rates and force out commission payments, leaving customers with nothing. We believe this is a short-sighted strategy that will not survive and that your interests are best served by utilizing the Mandatory Fee provision within the Order.

#### What Do You Need To Do?

There is nothing for you to do at this point. The Order has not yet been published in the Federal Register and the appeal process is still outstanding and to be determined. We do not need to modify any contracts at this point. Securus will contact you in the future if change of law provisions must be discussed and enacted.

#### Our Commitment To You Remains Unchanged

The work you do is extremely important and is the cornerstone of our nation's public safety policy. Securus Technologies will continue to be an advocate for you and our dedication to you will not change. We will continue to evaluate our options for appeal. However, if the Order does become effective, we do not plan to eliminate service from any location or significantly reduce any service levels due to its implementation. You have our promise on this.

While we will need to reduce future spending and capital investment, Securus is in a good position relative to the rest of our industry. Given our diversification across other lines of business, only about 60% of our revenue is associated with inmate telephone service, and profits and future growth from our subsidiaries will help us manage through these changes. Further, our future costs will be reduced given that we own our platform and technologies and don't need to pay third parties its use. Finally, our scale and past investment in our platform will also make us more efficient. Our commitment to you is that we will still be here and will still be supporting the necessary and important work that you do.

#### Questions?

We'll keep you updated with information regarding the implementation of this Order. Along the way, if you have questions or concerns, please contact your Securus Account Manager, or feel free to call me at 972-277-0386 or email me at [bpickens@securustechnologies.com](mailto:bpickens@securustechnologies.com).

Sincerely,



Robert Pickens  
President, Securus Technologies, Inc.

## **Fact Sheet of Inmate Rate Order**

### **The Order has yet to be published in the Federal Register.**

- Order is effective 90 days after publication in the Federal Register for Prisons
- Order is effective six months after publication in the Federal Register for Jails

**FCC is attempting to make sure that rates are just, reasonable and fair by establishing caps on all intrastate and interstate inmate calling rates and seeks only to include the costs of providing basic security features within the rate caps. The rate caps are as follows:**

- 11 cents/minute for debit and prepaid calls in state or federal prisons
- 14 cents/minute for debit and prepaid calls in jails with 1,000 or more inmates
- 16 cents/minute for debit and prepaid calls in jails with 350-999 inmates
- 22 cents/minute for debit and prepaid calls in jails up to 349 inmates
- Rates for collect calls are slightly higher in the first year and will be phased down to these rate caps over a two year transition period
- Eliminates the ability to subsidize lower rates with higher rates elsewhere

### **Ancillary service fees are capped in some cases and banned in many others.**

- Automated payment by phone or website: \$3
- Payment through a live agent: \$5.95
- Paper bill fee: \$2
- Third-party financial transaction fees, such as fees charged by MoneyGram or Western Union, may be passed through with no mark-up
- Prohibits all other ancillary service charges
- Allows for Mandated and Authorized Fees from a government body

### **The FCC strongly discourages "site commission" payments.**

- Excluded the cost of site commissions in establishing the rate caps and set rates below costs to effectively eliminate commissions
- The FCC will **monitor compliance annually and make further downward adjustment in rates, if providers are paying commissions**
- Defines the term "site commission" broadly and includes payments for anything unrelated to actual costs to provide basic service

### **The Order facilitates access for people with disabilities**

- Requires providers to offer free access to telephone relay service (TRS) calls for inmates with communications disabilities and applies a steeply discounted rate for TTY-to TTY calls
- Reminds correctional institutions of their obligation to make TRS available to people with communications disabilities
- Encourages jails and prisons to allow commonly used forms of TRS and requires them to report service quality issues

### **The FCC will provide extensive oversight and monitoring**

- To monitor compliance, inmate telephone providers are required to file data annually with information on rates, fees, site commission payments, etc.
- To ensure transparency for consumers, providers must disclose rates and fees
- The FCC is committed to closely monitoring the implementation of reforms, including a review in two years to determine if additional adjustments are required

**EXHIBIT C**

# Prison Phone Company Fights To Keep Profiting Off Inmates And Their Families

by Ben Walsh 2 min read [original](#)



Charlie Riedel/Associated Press Securus Technologies, a prison phone company, is pushing back against a proposed FCC regulation that would limit the amount it can charge inmates and their families for phone calls.



WASHINGTON -- Each month, Cesia Pineda spends between \$200 and \$250 to talk to her husband on the phone.

Normally, the calls would cost a tiny fraction of that, but Pineda's husband is an immigrant detainee at Stewart Detention Center in Lumpkin, Georgia, and he can't shop around for a cheaper plan. Securus Technologies, one of the nation's largest prison phone companies, is his only choice.

The Pinedas pay \$5.25, plus a \$6.25 processing fee that is added to every transaction, to talk for

20 minutes. These rates and fees are the norm in the multi-billion dollar prison phone industry, which has turned simple landline phone calls into an absurdly expensive proposition for inmates and their families.

Now the Obama administration wants to cap the rates and fees companies charge for prison phone service -- and Securus and its allies are fighting back. On Thursday, the Federal Communications Commission, which is controlled by Obama appointees, will vote on a [proposed rule](#) that would cap the vast majority of prison phone rates at 11 cents a minute and limit add-on fees, a major source of revenue for prison phone companies.

Securus, whose [earnings jumped](#) from \$87 million in 2013 to \$114.6 million last year, has warned that the publicly released proposal has “business-ending aspects” -- and said it and other companies would [threaten legal action](#) to block the new rules.

The warning stands in sharp contrast to a statement Securus made six months ago, when the company told [potential lenders](#) that it expected “the FCC’s Final Order to be neutral to modestly positive” to its earnings.

Here's what changed.

Securus and similar companies paid prisons [\\$460 million](#) in commissions in 2013 -- payments that Sens. Cory Booker (D-N.J.), Bernie Sanders (I-Vt.) and 14 other Democrats said last Thursday amounted to [kickbacks](#) to win contracts.

Prison officials love commissions, which help pad their budgets. But the biggest prison phone companies didn't like sending ever-increasing amounts of money to prison administrators. The companies were hoping the FCC would fix that problem for them.

In a [2014 letter](#), the three biggest prison phone firms suggested the FCC either ban or cap commissions -- which would have allowed the companies to blame the agency for slashing or eliminating payments to the prisons.

“This commission monster was constructed by the prison and jail telephone industry, which now wants the FCC to ride in, slay the beast, and bear the brunt of the facilities’ anger,” Peter Wagner, the executive director of the Prison Policy Initiative, said [in a filing](#) this January.

But the proposed rule, which is still being finalized, stops short of banning commissions. Instead, it “discourages” them -- and doesn't allow the prison phone companies to count them as legitimate costs they can pass on to prisoners.

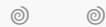
“I like this ruling a lot,” Wagner told The Huffington Post, referring to the public proposal. “It’s going to make the price of the calls reasonable and it’s going to address the fee problem. And I think the FCC’s approach is very good and comprehensive.”

Securus maintains that the new FCC regulation could be a "[business ending event](#)." But it's already taking steps to adjust to the new reality. After a 2013 interim regulation, it [stopped paying](#) commissions on interstate calls. That ensured that a higher percentage of the inflated rates Securus charges went to Securus -- and not to prison officials.

But it didn't save families like the Pinedas a cent. They'll have to wait until at least late January, the earliest the rate caps would go into effect.

Securus did not respond to requests for comment.

*Dana Liebelson and Roque Planas contributed reporting.*



**EXHIBIT D**

Solutions (<http://www.knowledgecenter/blog/industry-news-releases>) (<http://www.prnewswire.com/news-releases>) (<https://portal.prnewswire.com>)

See more news releases in

Computer Electronics (<http://www.prnewswire.com/news-releases/consumer-technology-latest-news/computer-electronics-list/>)

Telecommunications Industry (<http://www.prnewswire.com/news-releases/telecommunications-latest-news/telecommunications-industry-list/>)

Legal Issues (<http://www.prnewswire.com/news-releases/policy-public-interest-latest-news/legal-issues-list/>)

## Securus Provides Updates on Investigation into Stolen Data Records



Securus Technologies Inc.

DALLAS, Nov. 13, 2015 /PRNewswire/ -- Dallas, TX. – Securus Technologies continues to coordinate with law enforcement to investigate stolen data that was apparently provided to online outlet The Intercept according to the outlet's report on November 11, 2015.

Securus takes this matter very seriously, and is working on multiple fronts to fully investigate the matter and to prevent future criminal attacks. In addition to reporting the situation to the FBI, Securus has retained a forensic data analysis firm to conduct a thorough review of all systems and procedures to verify how this particular incident occurred and to confirm it happened outside of the Securus network and systems. The forensics experts will also recommend any steps to further secure all customer and inmate information.

While still ongoing, Securus can provide several updates and clarifications on the status of its investigation:

- All information we have gathered to this point indicates that data provided to The Intercept were from a single customer's data files and were likely accessed through a third-party vendor's file-sharing arrangement, unique to that customer. We have not seen what was provided to The Intercept beyond what they've reported, but there is no indication at this point that the theft involved any other customer's data nor that the data was obtained directly from the Securus network or platform.
- Despite allegations from The Intercept and other parties, we have seen no evidence to date of any attorney-client privileged communications that were recorded in error. While The Intercept reports that they matched call data from the

stolen data with phone numbers attached to attorneys' offices, no evidence has been provided that any of these calls were actually recorded, and if so, whether any of them would actually constitute privileged communications. Many calls from facilities are placed daily to law firms that are not subject to attorney client privilege including scheduling calls, informational queries, calls to people other than lawyers who work at law firms. There is a very important distinction between data that indicates that a call took place and an actual recording of the contents of that call. Data about the time and phone numbers of a call are generated for virtually every call that is placed in the U.S., and it is not covered by attorney-client privilege.

Our calling systems include multiple safeguards to prevent attorney-client recordings from occurring. Licensed attorneys are able to register their numbers or a specific call to exempt them from recording. Attorneys and inmates who do not register their numbers or calls will hear a warning about recording prior to the beginning of each call, and both must actively acknowledge they want to continue the call.

While it is possible that not all of these safeguards were followed by the callers in some cases, we have seen no evidence to date of recorded calls that would fall under that category. Without direct access to the stolen information, Securus cannot confirm whether any such recorded calls exist. If such evidence exists, we encourage The Intercept or other parties with access to the stolen data to provide that information to the FBI.

- Contrary to some reports, Securus does not sell call recordings or information to our law enforcement or correctional customers or anyone else. We record calls and provide forensic software to our customers based on the stipulations of our service contracts and in accordance with federal, state and local laws. Retention of these records is also conducted according to laws in various jurisdictions.
- No credit card data, financial information, social security numbers or similar data from any party was contained in the information that was stolen. While this fact was never in question, we have received multiple questions on this front. Securus does not store credit card information.

Securus is fully committed to completion of a full investigation into this matter. We will use the results of the investigation to enhance the security of our operations wherever possible to help ensure that a similar situation does not occur in the future. We will provide updates as new information becomes available.

Logo - <http://photos.prnewswire.com/prnh/20100831/DA57799>LOGO

SOURCE Securus Technologies

---

**EXHIBIT E**

# Announcing a new FCC.gov

## Tell us what you think and help shape the future »



[Search](#) | [RSS](#) | [Updates](#) | [E-Filing](#) | [Initiatives](#) | [Consumers](#) | [Find People](#)

### CPNI Template Submission

[Customer Proprietary Network Information \(CPNI\) Certification Home](#)

## Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template EB Docket 06-36

Submission Confirmation Number: **15178455**

Annual 64.2009(e) CPNI Certification for 2015 covering the prior calendar year:

1. Date filed:

2. Name of company(s) covered by this certification: 

- Securus Technologies, Inc. (818026)

3. Form 499 Filer ID(s):

4. Name of signatory:

5. Title of signatory:

6. Certification:

I,  [name of officer signing certification], certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company [☐ has ☒ has not] taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. [NOTE: If you reply in the affirmative, please provide an explanation of any actions taken against data brokers.]


The company [☐ has ☒ has not] received customer complaints in the past year concerning the unauthorized release of CPNI [NOTE: If you reply in the affirmative, please provide a summary of such complaints. This summary should include number of complaints, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not

authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed: [ ☒ Signature of an officer, as agent of the carrier]

**Attachments:** Accompanying Statement explaining CPNI procedures  
Explanation of actions taken against data brokers (if applicable)  
Summary of customer complaints (if applicable)

  
[STI CPNI Attachment 2015.pdf](#)

[Return to CPNI Home](#)

**Attachment 1**

Securus Technologies, Inc. ("Securus" or the "Company"), offers telecommunications services to law enforcement agencies and to inmates at confinement facilities, including the ability for inmates to complete interstate and international prepaid and collect calls ("inmate calling services"), pursuant to contracts that the Company enters with the administrators of the individual facilities.

To the extent that Securus collects any customer proprietary network information ("CPNI") in providing such services, the Company has internal procedures in place to ensure the security of the data, including its retention in secure password-protected files and other network access security measures. Employees are trained and understand the requirements to keep such information confidential.

Any such information is not sold, rented or otherwise made available to third parties, except to the extent permitted by applicable law and regulation (e.g., 47 U.S.C. 222(d)), including to ensure that inmates do not make fraudulent, abusive or illegal use of telecommunications privileges afforded by the confinement facility administrators.

Securus does not make CPNI available to its sales personnel and does not use, disclose or permit access to CPNI for internal marketing purposes (i.e., for the marketing among classes of services). Securus does make CPNI available to law enforcement agencies in connection with assorted services offered to law enforcement agencies, including services that allow law enforcement agencies to obtain the approximate geographical location of a called party. In cases in which a warrant or other lawful order is provided to Securus, Securus provides the relevant CPNI to law enforcement agencies in compliance with the applicable warrant or order.


Securus's Vice President, General Counsel and Secretary, Dennis Reinhold, understands the FCC CPNI Rules govern Securus's use and control of any CPNI purposes.

**ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF  
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2015:	Covering calendar year 2014
Name of company(s) covered by this certification:	Global Tel*Link Corporation
Form 499 Filer ID:	809240
Name of signatory:	Teresa Ridgeway
Title of signatory:	Secretary and Senior Vice President Administration

1. I, Teresa Ridgeway, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. §64.2001 *et seq.*
2. Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in §64.2001 *et seq.* of the Commission's rules.
3. The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year.
4. The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.
5. The company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

  
\_\_\_\_\_  
Teresa Ridgeway  
Secretary and Senior Vice President Administration  
Global Tel\*Link Corporation

February 19, 2015  
\_\_\_\_\_  
Date

**Attachment A**  
**Statement of CPNI Procedures and Compliance**

**Statement of CPNI Procedures and Compliance  
For CY2014  
Global Tel\*Link Corporation**

Global Tel\*Link Corporation operates as an inmate service provider and public payphone provider and as such, provides only operator-assisted call completion services for transient end users. Therefore, all of our services consist of casual traffic provided outside of any subscribed service relationship. We do not have any information that relates to the quantity, technical configuration, type, or location of the customer's presubscribed services. Because our service is provided outside of any presubscribed service relationship, we do not obtain any CPNI that can be used for marketing purposes.

Our marketing efforts are directed only toward correctional facilities and public payphone spaces, and such efforts do not include the use of CPNI. Should we expand our business in the future to include the provision of services that involve CPNI, we will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed, that it implements authentication procedures that do not require the use of readily available biographical information or account information, that it notifies customers of account changes, and informs law enforcement in the event of a breach of customer CPNI.

As set forth below, we have processes in place to safeguard call detail information from improper use or disclosure by employees, and to discover and protect against attempts by third parties to gain unauthorized access to call detail.

We do provide call detail information over the telephone. However, there are safeguards in place to protect against disclosure to unauthorized persons. We do not offer on-line access to CPNI. All customer service personnel are trained not to discuss call detail information unless the caller provides the appropriate password or date and time of the call in question, and we can verify it against our records. Customer service personnel must learn our company privacy policy and CPNI policy thoroughly, including the spectrum of consequences for violation, which spans from the issuance of a verbal warning up to the exercise of employee termination.

All of our accounts are kept anonymous. Customers must set up a pass code for use during billing inquiries. If a pass code is lost or forgotten, we have a back-up authentication method that does not involve the use of readily available biographical information. The customer must answer questions that only he or she would know. Otherwise the customer must provide a new pass code via fax or else requests for call detail are provided only by calling the customer back at the telephone number of record. We do not initiate changes to customer account information.

Our automated IVR allows end users to access only their account balance by providing their destination telephone account number (or pass code, if the customer has elected to use that option.) Call detail information is not provided through our automated IVR.

We have had no occasions where CPNI was disclosed to third parties, and we do have procedures in place to maintain records of any such disclosures. Any requests for call detail by outside parties must be accompanied by a court-ordered subpoena or search warrant, or clearance from the correctional facility that owns the records.

GTL has no retail locations and therefore does not disclose CPNI in-store.

We have procedures in place to notify law enforcement in the event of a confirmed breach of the call detail records. We have not had any such breaches during 2014, but we have a process in place to maintain records of any breaches discovered and notifications made to the USSS and the FBI.

We have not taken any actions against data brokers in the last year.

We did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2014.

Due to the nature of the specialized services GTL provides, the call detail we have is not tied to any presubscribed customers. Accordingly, we have not developed any information with respect to the processes pretexters may use to attempt to access CPNI.

**EB Docket 06-36**

Date \_\_\_\_\_

**Attachment A**  
**Statement of CPNI Procedures and Compliance**

**Statement of CPNI Procedures and Compliance  
For 2014  
Inmate Calling Solutions, LLC d/b/a ICSolutions**

Inmate Calling Solutions, LLC ("ICS") operates primarily as an inmate telephone service provider and, as such, provides only automated-operator assisted call completion services for transient end users. Therefore, all of its telephone services consist of casual traffic provided without any presubscribed service relationship. ICS does not have any information that relates to the quantity, technical configuration, type, or location of the consumer's subscribed telecommunication services. Moreover, ICS does not, in the ordinary course, obtain any CPNI that could be used for marketing purposes. Calls are either billed by the consumer's local exchange carrier or provided on a prepaid basis.

ICS' marketing efforts are directed only towards correctional facilities, and such efforts do not include the use of CPNI. Should ICS expand its business in the future to include the provision of services that involve CPNI, it will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure: (i) that notification is provided and consumer approval obtained before CPNI is used or disclosed, (ii) that it implements authentication procedures that do not require the use of readily available biographical information or account information, (iii) that it notifies customers of account changes, and (iv) that it informs law enforcement in the event of a breach of customer CPNI.

ICS has processes in place to safeguard call detail information from improper use or disclosure by employees, and to discover and protect against attempts by third parties to gain unauthorized access to call detail. ICS does not provide call detail information over the telephone. All customer service personnel are trained not to discuss call detail information unless the caller provides date and time of the subject call and they can verify same against ICS' records. For collect calls, the called party's local phone company bills the call charges on ICS' behalf and has its own controls for disclosure and access to applicable information.

For called parties who establish a prepaid account, ICS typically obtains customer name, address, and phone number in order to establish the account. However, since its telephone services are based on contractual relationships directly or indirectly with correctional facilities, ICS does not market any telephone services directly to consumers and, therefore, any information that could be deemed CPNI is only used for account administration purposes.

ICS' contracts with correctional facilities generally provide that call detail is the sole property of the correctional facility and that ICS must only disclose or allow access to this data by a) authorized correctional facility personnel, b) the paying party for billing purposes, or c) applicable ICS personnel for technical and billing support purposes. Correctional facility and ICS personnel must have a valid user ID and password in order to access this data at any time. Such personnel are assigned User IDs and passwords to enable controlled access to call detail records and recordings for inmate calls placed from the facility with which they are associated. For facility personnel, this access is handled on-site only by an authorized facility administrator. The administrator at each location will also establish and manage the process for any lost password replacement. The system provides for a password expiration which forces users to modify their password on a regular basis for added security. Passwords are not assigned based on readily-available biographical information.

Any other requests for call detail by outside parties are referred to designated management personnel at the correctional facilities who are themselves representatives of state and/or local law enforcement and, therefore, operate under applicable jurisdictional policies. Direct third party requests for call record detail must be made subject to a subpoena or other court sanctioned process.

As an inmate telephone service provider, ICS does not have any retail locations and therefore does not disclose CPNI on any "in-store" basis.

ICS has procedures in place to notify law enforcement in the event of a breach of the call detail records. Since ICS' customers are law enforcement entities, ICS defers to such entities for any escalation to federal agencies. ICS has not experienced any such breaches during 2014, but has a process in place to maintain records of any such breaches if/when discovered.

ICS has not taken any actions against data brokers in the past year.

ICS did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2014.

Due to the nature of the inmate calling service business, the underlying call detail is not tied to any presubscribed customers. Accordingly, ICS has not developed any information with respect to the processes that pretexters may use to attempt to access CPNI.

# Announcing a new FCC.gov

## Tell us what you think and help shape the future »

[Search](#) | [RSS](#) | [Updates](#) | [E-Filing](#) | [Initiatives](#) | [Consumers](#) | [Find People](#)

### CPNI Template Submission

[Customer Proprietary Network Information \(CPNI\) Certification Home](#)

## Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template EB Docket 06-36

Submission Confirmation Number: **71515214**

Annual 64.2009(e) CPNI Certification for 2015 covering the prior calendar year: **2014**

1. Date filed: **Jul 17 2015 3:49PM**
2. Name of company(s) covered by this certification:
  - **Telmate LLC (828639)**
3. Form 499 Filer ID(s): **828639**
4. Name of signatory: **Scott Lam**
5. Title of signatory: **General Counsel**
6. Certification:

I, **Scott Lam** [name of officer signing certification] , certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company [ ☐ has ☒ has not] taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. [NOTE: If you reply in the affirmative, please provide an explanation of any actions taken against data brokers.]

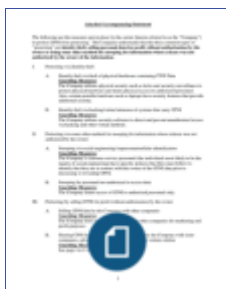
The company [ ☐ has ☒ has not] received customer complaints in the past year concerning the unauthorized release of CPNI [NOTE: If you reply in the affirmative, please provide a summary of such complaints. This summary should include number of complaints, broken down by category or

complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed: [ ☒ Signature of an officer, as agent of the carrier]

**Attachments:** Accompanying Statement explaining CPNI procedures  
Explanation of actions taken against data brokers (if applicable)  
Summary of customer complaints (if applicable)



[Telmate CPNI - Accompanying Statement.pdf](#)

[Return to CPNI Home](#)

---

[FCC Home](#) | [Search](#) | [RSS](#) | [Updates](#) | [E-Filing](#) | [Initiatives](#) | [Consumers](#) | [Find People](#)

---

Federal Communications Commission Phone: 1-888-CALL-FCC  
445 12th Street SW (1-888-225-5322)  
Washington, DC 20554 TTY: 1-888-TELL-FCC  
[More FCC Contact Information...](#) (1-888-835-5322)  
Fax: 1-866-418-0232  
E-mail: [fccinfo@fcc.gov](mailto:fccinfo@fcc.gov)

- [Privacy Policy](#)
- [Website Policies & Notices](#)
- [Required Browser Plug-ins](#)
- [Freedom of Information Act](#)

CPNI Template Submission Software Version 00.01.03 April 5, 2011

## Attached Accompanying Statement

The following are the measures put in place by the carrier (herein referred to as the “Company”) to protect CPNI from pretexting. The Company understands that the three common types of “pretexting” are **identity theft, selling personal data for profit without authorization by the owner or using some other method for snooping for information whose release was not authorized by the owner of the information.**

I. Pretexting via identify theft

A. Identify theft via theft of physical hardware containing CPNI Data

**Guarding Measures:**

The Company utilizes physical security such as locks and security surveillance to protect physical hardware and limits physical access to authorized personnel. Also, certain portable hardware such as laptops have security features that provide additional security.

B. Identify theft via hacking/virtual intrusion of systems that carry CPNI

**Guarding Measures:**

The Company utilizes security software to detect and prevent unauthorized access via hacking and other virtual methods.

II. Pretexting via some other method for snooping for information whose release was not authorized by the owner

A. Snooping via social engineering/ impersonation/false identification

**Guarding Measures:**

The Company’s customer service personnel (the individuals most likely to be the targets of social engineering) have specific policies that they must follow to identify that they are in contact with the owner of the CPNI data prior to discussing or revealing CPNI.

B. Snooping by personnel not authorized to access data

**Guarding Measures:**

The Company limits access of CPNI to authorized personnel only.

III. Pretexting by selling CPNI for profit without authorization by the owner

A. Selling CPNI data by the Company with other companies

**Guarding Measures:**

The Company does not share CPNI data with other companies for marketing and profit purposes.

B. Sharing CPNI data for profit/marketing purposes by the Company with sister companies, subsidiaries, parent companies or joint venture entities

**Guarding Measures:**

See page 4 to 8 for details (items 1 to 18).

### **Attached Accompanying Statement**

The following items (1) to (18) are how the Company guards CPNI against pretexting in the form of selling CPNI for profit or marketing purposes by the Company to its sister companies, subsidiaries, parent companies or joint venture entities but without authorization by the owner. In the event that the Company was to sell or share CPNI with its affiliated entities for marketing or profit purposes, it would strictly abide by the following policies in compliance with FCC rules as outlined in section 222 of the Communications Act of 1934 as amended, 47 U.S.C. 222 (47 C.F.R. § 64.2001 to 64.2011 et seq.).

#### **How The Company Complies with 47 C.F.R. § 64.2001-64.2011 et seq.**

1. The Company does not enable use, disclosure or permit access to CPNI for any marketing purposes to any persons, entities parties outside of the Company without the specific consent of the customer that owns the CPNI data.
2. If the Company wishes to share CPNI with any subsidiaries or parent companies of the Company and the customer only subscribes to only 1 category of service offered by the Company, the Company will secure the consent of the customer prior to sharing that CPNI data with subsidiaries or parent companies of the Company.
3. In most cases, the Company will go a step above and try to secure the consent of the customer to share CPNI data with subsidiaries and parent companies of the Company, regardless of whether customer subscribes to 1 or more than 1 type of service offered by the Company.
4. The Company will not utilize, disclose or permit access to CPNI data to identify or track customers that call competing service providers.
5. If the Company requires customer consent for utilizing, disclosing or permitting access to CPNI data, the Company will obtain consent through written, oral or electronic methods.
6. The Company understands that carriers that rely on oral approval shall bear the burden of proving that such approval has been given in compliance with the Commission's rules.
7. The Company has a policy in which any customer approvals obtained for the use, disclosing or utilization of CPNI data will remain in effect until the customer revokes or limits such approval or disapproval.
8. For all Opt-Out and Opt-In Approval Processes utilized by the Company in which the CPNI data is used for marketing communications related services to that customer, the Company will make that customer's data individually identifiable to the customer and state the specific marketing purpose that CPNI would be utilized.

### Attached Accompanying Statement

9. Prior to any solicitation of the customer for approval, the Company provides notification to the customer of the customer's rights to restrict to use of, disclosure of, and access to that customer's CPNI.
10. The Company maintains records of- notification, whether oral, written or electronic, for at least one year. The Company provides individual notices to customers when soliciting approval to use, disclose or permit access to customer's CPNI.
11. In cases where the Company requests CPNI release requests from the customer, the Company includes the following in its "**Consent of Notice**"
  - a. Sufficient information to enable the customer to make an informed decision as to whether to permit the Company to use, disclose or permit access to, the customer's CPNI.
  - b. Statement declaring that the customer has a right, and that the Company has the duty, under federal law, to protect the confidentiality of CPNI.
  - c. Specific statement on that the types of information that constitute CPNI (as defined in 64.2001) and the specific entities that will receive the CPNI, describing the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.
  - d. Statement advising the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and clear statement that a denial of approval will not affect the provision of any services to which the customer subscribes. The Company also provides a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI. The Company's notification will be comprehensible and not be misleading.
12. "**Consent of Notice**" (continued from page 4...)
  - a. In cases where the Company utilizes written notification, the notice will be clear, legible, sufficiently large type and be placed in an area so as to be readily apparent to a customer.
  - b. In the event that the notification is to be translated into another language, then all portions of the Company's notification will be translated into that language.
  - c. The Company will not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.


### **Attached Accompanying Statement**

- d. The notification will state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from the Company is valid until the customer affirmatively revokes or limits such approval or denial.
  - e. The Company's solicitation for approval will state the customer's CPNI rights (defined in 47 C.F.R. § 64.2001 to 64.2011 et seq.).
- 13. All of the Company's notices specific to Opt-Out option will be provided via electronic or written notification. The Company will not utilize purely oral notification.
- 14. The Company must wait a minimum of 30 days after giving customer notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. The Company may, in its discretion, provide for a longer period for notification and opportunity for opt-out option. The Company does notify customers as to the applicable waiting period for response before approval is assumed. The Company also abides by the following as far as minimum waiting period.
  - a. In cases where the Company utilizes electronic notification, the Company's waiting period begins to run from the date that the notification was mailed.
  - b. In the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.
- 15. The Company's opt-out mechanism will provide notices to the customer every two years.
- 16. The Company will ensure that all notifications will comply with the requirements listed above but recognizes that under FCC CPNI rules enable the Company to omit any of the following notice provisions if not relevant to the limited use for which the Company seeks CPNI:
  - a. Under the applicable FCC CPNI rules, The Company recognizes that it will not need to advise customers that if they opted-out previously, no action is needed to maintain the opt-out election.
  - b. The Company also recognizes that it need not advise customers that they may share CPNI with the affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party;

**Attached Accompanying Statement**

- c. The Company recognizes that it need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as the Company explains to customers that the scope of the approval the carrier seeks is limited to one-time use.
- d. The Company recognizes that it may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the Company clearly communicates that the customer can deny access to his CPNI for the call.

EB Docket 06-36

  
Vincent Townsend, CEO  
Pay Tel Communications, Inc  
2/23/15  
Date

**Attachment A**  
**Statement of CPNI Procedures and Compliance**

## **PAY TEL COMMUNICATIONS, INC.**

**2014**

### **STATEMENT OF CPNI PROCEDURES AND COMPLIANCE**

Pay Tel Communications, Inc. operates as an institutional service provider offering operator-assisted call completion services for use by inmates and other incarcerated persons pursuant to contract with confinement facilities. All of our services consist solely of casual traffic provided outside of any subscribed service relationship. We do not have any information that relates to the quantity, technical configuration, type, or location of the called party's presubscribed services. Because our service is provided outside of any presubscribed service relationship, we do not obtain any Customer Propriety Network Information (CPNI) that can be used for marketing purposes.

Our marketing efforts are directed only toward the confinement facilities and such efforts do **not** include the use of any end user's personal information or telephone call detail. Should we expand our business in the future to include the provision of services that involve CPNI, we will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed, that it implements authentication procedures that do not require the use of readily available biographical information or account information, that it notifies customers of account changes, and informs law enforcement in the event of a breach of customer CPNI.

As set forth below, we have processes in place to safeguard call detail information from improper use or disclosure by employees, and to discover and protect against attempts by third parties to gain unauthorized access to call detail.

Pay Tel has safeguards in place to protect against disclosure of call detail information to unauthorized persons. Pay Tel does not disclose call detail information in response to customer-initiated telephone contact or online access, unless the customer provides the appropriate personal identification number (PIN) for the prepaid account in question, and we can verify it against our records. All customer service personnel are trained not to discuss call detail information unless the caller provides the required PIN. Customer service personnel must learn our company privacy policy and CPNI policy thoroughly. Violation of these policies subjects the employee to disciplinary action, up to and including immediate dismissal.

If a PIN is lost or forgotten, we have a back-up authentication method that does not involve the use of readily available biographical information. The customer must establish a new PIN via Pay Tel's website or provide proof of identity via fax or US Mail. Proof of identify must include a copy of the customer's driver's license and most recent bill or statement. We do not initiate changes to customer account information.

We have had no occasions where call detail or CPNI was disclosed to third parties, but we do have procedures in place to maintain records of any such disclosures. Any requests for call detail by outside parties must be accompanied by a court-ordered subpoena or search warrant, or clearance from the correctional facility that owns the records.

Pay Tel has no retail locations and therefore does not disclose CPNI in-store.

We have procedures in place to notify law enforcement in the event of a confirmed breach of the call detail records. We have not had any such breaches during 2014, but we have a process in place to maintain records of any breaches discovered and notifications made to the USSS and the FBI.

We have not taken any actions against data brokers in the last year.

We did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2014.

Due to the nature of the specialized services Pay Tel provides, the call detail we have is not tied to any presubscribed customers. Accordingly, we have not developed any information with respect to the processes pretexters may use to attempt to access CPNI.

**EXHIBIT F**



## **GTL's Location IQ™ Gives Correctional Facilities Insight by Pinpointing Called Party Location**

*Industry tech leader announces patent-pending intelligence application to combat criminal activity*

Reston, VA ([PRWEB](#)) June 25, 2015 -- Global Tel\*Link (GTL), the leading provider of correctional technology solutions, announces the release of Location IQ™, a new, patent-pending intelligence application available for its inmate telephone platforms that combats fraud and other criminal activity. Additionally, this technology ensures adherence to facility regulations by pinpointing the location of a called party device receiving calls from a correctional facility.

Using powerful, accurate carrier tower- and GPS-based location services, GTL's Location IQ identifies the called party's location regardless of the network or device type. Location IQ offers correctional facilities the ability to identify the location of a mobile device that has accepted a call from a correctional facility, offering both latitude/longitude coordinates and proximity to the given facility. Through the inmate telephone platform's graphical user interface, investigators are provided a map showing the location of the phone in a readily accessible and usable format.

As an added control feature, protocols can be implemented so that if a specific call is within a pre-established perimeter of the facility, the call can be blocked from connecting. Alternatively, investigators have the option of allowing the call to continue while monitoring and recording the call in real time, thus providing investigators valuable information about the suspicious call. This helps investigators to combat criminal activity, such as attempted escapes or the bringing of contraband items into a facility, by blocking calls between inmates and parties in close proximity to the correctional facility, many of which are located in remote areas. Location IQ is also beneficial to support court orders that may be required for on-demand cell phone locations.

Location IQ is one of many tools in the IQ family of intelligence products. Together, these products form the most holistic approach to intelligence gathering in the correctional industry, offering investigators a broad range of options for gathering pertinent, actionable intelligence. Location IQ and other innovations from GTL will be showcased June 29-30 in booth 1100 at the National Sheriffs' Association's Annual Conference and Exhibition in Baltimore, Maryland.

For more information about this new investigative feature, contact a GTL representative today for a demonstration or visit [www.gtl.net/locationiqpr](http://www.gtl.net/locationiqpr).

###

### **About Global Tel\*Link**

GTL is the leading provider of integrated correctional technology solutions, delivering financial value, security, and ease of operation to our customers through visionary products and solutions at the forefront of corrections innovation. As a trusted correctional industry leader, GTL provides service to approximately fifty percent of inmates nationwide, including service to 33 state departments of corrections, the District of Columbia, Puerto Rico, and 32 of the largest city/county facilities. GTL is headquartered in Reston, Virginia, with more than 10 regional offices across the country. To find out more about GTL, please visit our website [www.gtl.net](http://www.gtl.net).



Telmate's investigator toolkit is a powerful, technologically-advanced suite of tools that provides actionable intelligence helping law enforcement to prevent and solve crime.

With Telmate Investigator, facilities can instantly analyze inmates' personal networks and gain unprecedented crime fighting intelligence.

**“In my 15 years of law enforcement, Telmate is by far the leading investigator tool. If you're a policeman and you're not using it, you are behind the times.”**

*Sergeant Jamie Harris  
Lake County Police  
Department Detective*



**Call Pattern Analysis**



**Call and Video Playback**



**Contact Analysis**



**Inmate & Contact Profiles**



**Communication Timeline**



**Voice & Image Biometrics**



**Cell Phone Data Extraction**



**3-Way Call Detection**



**Evidence Reporting**



**Relationship Analysis**



**Configurable Alarms and Alerts**



**Visualization Tools**



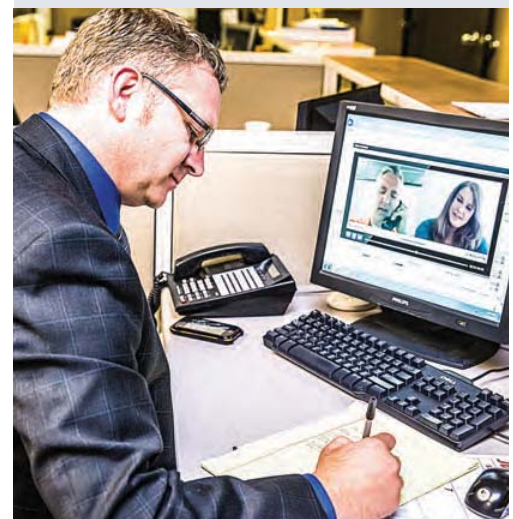
**Call Destination Mapping**



**Web Based Application**



**Live Call Monitoring**



## The Telmate Timeline: See the Life of a Resident

The Telmate Timeline compiles an inmate's booking, financial, and communication history into a single sortable history. All data can be filtered and sorted, and can easily be exported as PDF documents for trial exhibits. The Telmate Timeline combines:

**Booking Information** Where and when the resident was booked, including booking photo.

**Calls** Attempted and completed call recordings, as well as recipient detail and call duration.

**Voicemail** Includes the phone number and verified contact name and identity (with Telmate Verify).

**Video Visits** Complete recordings of video visits including the contact name and verified identity.

**Deposits** Time, place, amount and depositor details, including photos and address information.

## Connection Tool: Map Any Interaction Automatically

We know that investigators spend a huge amount of time combing through visitation logs, phone records and deposit records to determine who your residents are in contact with. Our connection tool leverages inmate communications activity with Telmate Verify to identify an inmate's personal networks and to highlight suspicious activity. This tool can even suggest potential connections where direct contact has not been made.

## 3-Way Call Handling

Telmate has the most comprehensive and accurate 3-way call detection system in the industry. Most automated 3-way detection systems either disconnect (and possibly block) a

large percentage of legitimate calls, or ignore a high number of 3-way events. With Telmate, suspected 3-way calls are automatically flagged as "3-way Suspected" and a clickable timecode is provided to quickly link investigators to the suspected point in the call. All suspected 3-way calls are reviewed by live Telmate operators in less than 5 minutes to ensure accuracy and eliminate false positives. It takes one of our live operators less than 5 minutes from the time of detection to review a suspected 3-way call.

## Cell Phone Data Extraction

Our advanced extraction technology is based on the same technology utilized by the FBI and DOD. With a warrant or consent, all inmate cell phone data can be easily extracted and seamlessly imported into Telmate Investigator for instant evaluation and analysis.



## Why Telmate?

### The Industry's Best Service and Support

We offer the industry's best customer service with live US-based, bi-lingual 24/7 toll-free support, in-house repair technicians, 24 hour circuit monitoring and two hour, on-site response time.

### Increase Usage and Operating Efficiencies

Our range of communications products, automated admin tasks and deposit options drive increased system usage and unsurpassed operating efficiencies.

### Innovative Technology

Our system is the most robust, full featured, and secure inmate communications platform available featuring deposit and account management, phone, video visits, social media, investigation tools, mobile access and full integration with commissary and JMS systems.

### Unified Software Platform

Telmate's fully integrated software and hardware ecosystem has been designed and built by our engineers to meet the unique needs of the corrections industry.

Telmate is one of the fastest growing inmate communications systems in North America currently providing service to hundreds of correctional facilities in nearly every U.S. State and four Canadian Provinces. From city and county jails to federal facilities, Telmate serves populations of all sizes—many exceeding 1,000 beds.

UPGRADE your inmate communications system to Telmate.  
sales@telmate.com | 1.855.TELMATE (835.6283)



**EXHIBIT G**

## INVESTIGATIVE SOLUTIONS > INVESTIGATION > **SECURUS LOCATION BASED SERVICES**

Inmate calls to cellular telephones represent a challenge to a facility's ability to know where inmate calls are going. Cellular telephone numbers can be anonymous and can be located anywhere, including just outside a facility. With the increasing trend across the United States to rely exclusively on cellular telephone service, facilities need to be able to ensure that security is not compromised.

Because of their mobility, cellular telephones are a favorite way for inmates to coordinate criminal activities, escapes, the introduction of contraband, and to conspire to hide evidence.

Securus' Secure Call Platform (SCP) includes support for Location Based Services (LBS), which provides facilities with the control and oversight needed to safeguard against these threats. LBS provides facilities with the following capabilities:

- Investigate, in hindsight, the location of inmate calls to cellular telephones
  - Leverage inmate call records to identify locations of investigative interest
  - Discover geographical connections between calls, inmates, and called parties
- Receive real-time alerts based on where the call is placed
  - Know when inmates are calling cellular telephones within a specific radius of your facility
  - Know when inmates are calling cellular telephones in an area of interest
  - Increase the precision of leads generated from other inmate calling alerts by only triggering when those calls are to cellular telephones in a geographic area of interest
- Find the location of a cellular telephone even if it is not currently involved with a call to an inmate, with appropriate authorization

### How LBS Works:

LBS works by collecting the approximate location of a cellular telephone, through the cellular provider, as soon as the called party accepts the call from the inmate. The originating location as well as the location of the cellular telephone at the end of the call is recorded and available for research and investigation.

LBS is not dependent on cellular telephone GPS settings, which can be turned off by users seeking to escape tracking. This is a great advantage, ensuring that your facility knows where your inmates are calling even when the billing name and address of the called party might not be known.

If you would like to learn more about LBS, contact us at

[Sales@securustechnologies.com](mailto:Sales@securustechnologies.com) (<mailto:Sales@securustechnologies.com?subject=SECURUS%20LOCATION%20BASED%20SERVICES>)

We exist to [serve](#) and [connect](#) to make our world safe.

“

Our facility has become one of the FBI Terrorism Task Force regular sources of information. We have monitored and burn thousands of minutes of copies of phone calls of inmates connected to Al-Quida that has resulted in the identification of terrorism cells in the New York area. I just wanted you to know that our entire country has benefited from the inmate phone monitoring service we have. I am glad we made the change and it has enhanced our security at our facility. ”

— Detention Center, Washington

**EXHIBIT H**

## INVESTIGATIVE SOLUTIONS > INVESTIGATION > **SECURUS THREADS™**

### Fuel Your Investigation and Identify FOCUSED LEADS NATIONWIDE!

Securus has partnered with top experts in investigative analysis and law enforcement to bring you the very best in data analytics. THREADS provides investigators with actionable intelligence and focused leads using data collected from a nationwide community! Securus' Secure Call Platform (SCP), combined with THREADS, is unequivocally the largest centralized data repository and most powerful analysis software on the market for both corrections and law enforcement.

Traditionally, communications data available for analysis by corrections and law enforcement has been limited to a specific facility or single investigator. This data typically resided on someone's computer or in software that only a few agents could use. This limitation caused delays or even hindered an investigation.

Now, nationwide, more than 400 law enforcement officers are using THREADS investigative software to uncover focused leads based on their targets/suspects. The THREADS database includes the following and continues to grow every day:

- More than 600,000 people with billing name and address (not incarcerated)
- More than 950,000 inmates
- More than 1,900 correctional facilities
- More than 100,000,000 call records between inmates and called parties

### Bridging the gap between Corrections and Law Enforcement

The THREADS platform brings to market a nationwide, investigative community that bridges the gap between law enforcement agencies and correctional facilities. THREADS allows investigators to reach from coast to coast to uncover focused leads in a matter of seconds. The data available for analysis includes that of any corrections facility enrolled in our nationwide community and residing on SCP.

### **THREADS also provides investigators with the capability to import external investigative data such as the following:**

- Cell forensics information from confiscated cell phones (text messages, emails,

### **THREADS Community Use Agreement**

Securus' THREADS platform brings to the market a nationwide investigative community, bridging the gap between law enforcement agencies and corrections facilities. This allows investigators to reach coast to coast to uncover focused leads across the country in a matter of seconds. The data available for analysis is that of any corrections facility enrolled in the nationwide community and residing on the most powerful communications platform SCP, as well as any information imported into the community by users across the country.

The default version of THREADS will provide you with powerful analytics using only the data related to your corrections facility. However, to join the community and put THREADS to work for you analyzing data nationwide, please download and sign the THREADS Community Use Agreement and return to your Securus Account Executive.

Download Agreement (/documents/10603/11067/THREADS+Community+Use+Agreement.pdf/d49221d3-8155-473d-9c80-c74a6b1cb0d8)

- call records, contacts, pictures, etc.)
- Subpoenaed public phone records
- Cell tower dumps, which includes information an hour before and an hour after a crime occurred
- Pictures
- Mail
- Criminal events
- And much more

The THREADS platform takes full advantage of this vast amount of data to provide a centralized, nationwide system producing actionable intelligence and focused leads immediately upon install to investigators from coast to coast.

### **THREADS provides the following analytics:**

- Calling patterns
- Linkage analysis
- Inner circle identification (suspects' inner working group)
- Bounce list hit notifications (is the inmate calling someone on your staff?)
- Associations
- Chain dialing
- Interactive maps
- The most likely leader of a criminal organization
- And much more...

THREADS helps to determine a high probability of an inmate using a cellular telephone, and also allows for the information obtained from the cellular telephone (once confiscated) to be directly imported into THREADS making the data available for analysis along with the information already in THREADS and SCP to build targeted leads for investigators.

### **THREADS can also be used to help identify the following:**

- Detect patterns of fraternization between inmates and correctional officers, nursing, and/or commissary staff
- Discover common contacts between inmates and called parties
- Customize information and reporting to filter out irrelevant calls, such as girlfriends or legal counsel
- Detect criminal organizations being run from within the facility
- Find associations between multiple parties
- Identify inmates who possibly have a cellular telephone based on calling patterns and holes in communications

Join the community and put THREADS to work for you analyzing data nationwide, fill out, sign, and submit the Community Use Agreement (</documents/10603/11067/THREADS+Community+Use+Agreement.pdf/d49221d3-8155-473d-9c80-c74a6b1cb0d8>) to your Securus account representative today!



## Exhibit C: THREADS™ USE AGREEMENT KANKAKEE COUNTY SHERIFF'S DEPARTMENT (IL)

This THREADS™ Use Agreement is by and between Kankakee County Sheriff's Department ("Customer") and Securus Technologies, Inc., ("we," "us," or "Provider") and is part of and governed by the Master Services Agreement (the "Agreement") executed by the parties. The obligations set forth herein are in addition to and not in lieu of the terms and conditions of the Agreement, which are incorporated herein by reference. This THREADS™ Use Agreement shall be effective as of the last date signed by either party and shall be coterminous with the Agreement.

- 1. COMPLIANCE WITH APPLICABLE LAWS.** Customer will comply with all privacy, consumer protection, marketing, and data security laws and government guidelines applicable to Customer's access to and use of information obtained in connection with or through the THREADS™ application. Customer acknowledges and understands that the Customer is solely responsible for its compliance with such laws and that Provider makes no representation or warranty as to the legality of the use of the THREADS™ application or the information obtained in connection therewith. Provider shall have no obligation, responsibility, or liability for Customer's compliance with any and all laws, regulations, policies, rules or other requirements applicable to Customer by virtue of its use of the THREADS™ application.
- 2. SECURITY.** Customer acknowledges that the information available through the THREADS™ application includes personally identifiable information and that it is Customer's obligation to keep all such accessed information secure. Accordingly, Customer shall (a) restrict access to THREADS™ to those law enforcement personnel who have a need to know as part of their official duties; (b) ensure that its employees (i) obtain and/or use information from the THREADS™ application only for lawful purposes and (ii) transmit or disclose any such information only as permitted or required by law; (c) keep all user identification numbers confidential and prohibit the sharing of user identification numbers; (d) use commercially reasonable efforts to monitor and prevent against unauthorized access to or use of the THREADS™ application and any information derived therefrom (whether in electronic form or hard copy); (e) notify Provider promptly of any such unauthorized access or use that Customer discovers or otherwise becomes aware of; and (f) unless required by law, purge all information obtained through the THREADS™ application and stored electronically or on hard copy by Customer within ninety (90) days of initial receipt or upon expiration of retention period required by law.
- 3. PERFORMANCE.** Customer understands and acknowledges that all information used and obtained in connection with the THREADS™ application is "AS IS." Customer further understands and acknowledges that THREADS™ uses data from third-party sources, which may or may not be thorough and/or accurate, and that Customer shall not rely on Provider for the accuracy or completeness of information obtained through the THREADS™ application. Customer understands and acknowledges that Customer may be restricted from accessing certain aspects of the THREADS™ application which may be otherwise available. Provider reserves the right to modify, enhance, or discontinue any of the features that are currently part of the THREADS™ application. Moreover, if Provider determines in its sole discretion that the THREADS™ application and/or Customer's use thereof (1) violates the terms and conditions set forth herein and/or in the Agreement or (2) violates any law or regulation or (3) is reasonably likely to be so determined, Provider may, upon written notice, immediately terminate Customer's access to the THREADS™ application and shall have no further liability or responsibility to Customer with respect thereto.
- 4. WARRANTIES/LIMITATION OF LIABILITY.** Provider shall have no liability to Customer (or to any person to whom Customer may have provided data from the THREADS™ application) for any loss or injury arising out of or in connection with the THREADS™ application or Customer's use thereof. If, notwithstanding the foregoing, liability can be imposed on Provider, Customer agrees that Provider's aggregate liability for any and all losses or injuries arising out of any act or omission of Provider in connection with the THREADS™ application, regardless of the cause of the loss or injury, and regardless of the nature of the legal or equitable right claimed to have been violated, shall never exceed \$100.00. Customer covenants and promises that it will not seek to recover from Provider an amount greater than such sum even if Customer was advised of the possibility of such damages. PROVIDER DOES NOT MAKE AND HEREBY DISCLAIMS ANY WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO THE THREADS™ APPLICATION. PROVIDER DOES NOT GUARANTEE OR WARRANT THE CORRECTNESS, COMPLETENESS, LEGALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OF THE THREADS™ APPLICATION OR INFORMATION OBTAINED IN CONNECTION THEREWITH. IN NO EVENT SHALL PROVIDER BE LIABLE FOR ANY INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, HOWEVER ARISING, INCURRED BY CUSTOMER FROM RECEIPT OR USE OF INFORMATION OBTAINED IN CONNECTION WITH THE THREADS™ APPLICATION OR THE UNAVAILABILITY THEREOF.
- 5. INDEMNIFICATION.** Customer hereby agrees to protect, indemnify, defend, and hold harmless Provider from and against any and all costs, claims, demands, damages, losses, and liabilities (including attorneys' fees and costs) arising from or in any way related to Customer's use of the THREADS™ application or information obtained in connection therewith.

AGREED TO AND ACCEPTED:

<b>CUSTOMER:</b> Kankakee County Sheriff's Department  By: <u>Michael D. Downey</u> Name: <u>Michael D. Downey</u> Title: <u>Chief of Corrections</u> Date: <u>3/25/13</u>	<b>PROVIDER:</b> Securus Technologies, Inc.  By: <u>Robert Pickens</u> Name: <u>Robert Pickens</u> Title: <u>Chief Operating Officer</u> Date: <u>4-1-13</u>
--	--



## EXHIBIT D: LOCATION-BASED SERVICES USE AGREEMENT KANKAKEE COUNTY SHERIFF'S DEPARTMENT (IL)

This Location-Based Services Use Agreement is by and between Kankakee County Sheriff's Department ("Customer") and Securus Technologies, Inc. ("we," "us," or "Provider"), and is part of and governed by the Master Services Agreement (the "Agreement") executed by the parties. The obligations set forth herein are in addition to and not in lieu of the terms and conditions of the Agreement, which are incorporated herein by reference. This Location-Based Services Use Agreement shall be effective as of the last date signed by either party and shall be coterminous with the Agreement.

**1. COMPLIANCE WITH APPLICABLE LAWS.** Customer will comply with all privacy, consumer protection, marketing, and data security laws and government guidelines applicable to Customer's access to and use of information obtained in connection with or through the Location-Based Services application. Customer acknowledges and understands that the Customer is solely responsible for its compliance with such laws and that Provider makes no representation or warranty as to the legality of the use by Customer of the Location-Based Services application or the information obtained in connection therewith. Provider shall have no obligation, responsibility, or liability for Customer's compliance with any and all laws, regulations, policies, rules or other requirements applicable to Customer by virtue of its use of the Location-Based Services application.

**2. SECURITY.** Customer acknowledges that the information available through the Location-Based Services application includes personally identifiable information and that it is Customer's obligation to keep all such accessed information secure. Accordingly, Customer shall (a) restrict access to Location-Based Services to those law enforcement personnel who have a need to know as part of their official duties; (b) ensure that its employees (i) obtain and/or use information from the Location-Based Services application only for lawful purposes and (ii) transmit or disclose any such information only as permitted or required by law; (c) keep all user identification numbers confidential and prohibit the sharing of user identification numbers; (d) use commercially reasonable efforts to monitor and prevent against unauthorized access to or use of the Location-Based Services application and any information derived therefrom (whether in electronic form or hard copy); (e) notify Provider promptly of any such unauthorized access or use that Customer discovers or otherwise becomes aware of; and (f) unless required by law, purge all information obtained through the Location-Based Services application and stored electronically or on hard copy by Customer within ninety (90) days of initial receipt or upon expiration of retention period required by law.

**3. PERFORMANCE.** Customer understands and acknowledges that all information used and obtained in connection with the Location-Based Services application is "AS IS." Customer further understands and acknowledges that Location-Based Services uses data from third-party sources, which may or may not be thorough and/or accurate, and that Customer shall not rely on Provider for the accuracy or completeness of information obtained through the Location-Based Services application. Customer understands and acknowledges that Customer may be restricted from accessing certain aspects of the Location-Based Services application which may be otherwise available. Provider reserves the right to modify, enhance, or discontinue any of the features that are currently part of the Location-Based Services application. Moreover, if Provider determines in its sole discretion that the Location-Based Services application and/or Customer's use thereof (1) violates the terms and conditions set forth herein and/or in the Agreement or (2) violates any law or regulation or (3) is reasonably likely to be so determined, Provider may, upon written notice, immediately terminate Customer's access to the Location-Based Services application and shall have no further liability or responsibility to Customer with respect thereto.

**4. WARRANTIES/LIMITATION OF LIABILITY.** Provider shall have no liability to Customer (or to any person to whom Customer may have provided data from the Location-Based Services application) for any loss or injury arising out of or in connection with the Location-Based Services application or Customer's use thereof. If, notwithstanding the foregoing, liability can be imposed on Provider, Customer agrees that Provider's aggregate liability for any and all losses or injuries arising out of any act or omission of Provider in connection with the Location-Based Services application, regardless of the cause of the loss or injury, and regardless of the nature of the legal or equitable right claimed to have been violated, shall never exceed \$100.00. Customer covenants and promises that it will not seek to recover from Provider an amount greater than such sum even if Customer was advised of the possibility of such damages. PROVIDER DOES NOT MAKE AND HEREBY DISCLAIMS ANY WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO THE LOCATION-BASED SERVICES APPLICATION. PROVIDER DOES NOT GUARANTEE OR WARRANT THE CORRECTNESS, COMPLETENESS, LEGALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OF THE LOCATION-BASED SERVICES APPLICATION OR INFORMATION OBTAINED IN CONNECTION THEREWITH. IN NO EVENT SHALL PROVIDER BE LIABLE FOR ANY INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, HOWEVER ARISING, INCURRED BY CUSTOMER FROM RECEIPT OR USE OF INFORMATION OBTAINED IN CONNECTION WITH THE LOCATION-BASED SERVICES APPLICATION OR THE UNAVAILABILITY THEREOF.

**5. INDEMNIFICATION.** Customer hereby agrees to protect, indemnify, defend, and hold harmless Provider from and against any and all costs, claims, demands, damages, losses, and liabilities (including attorneys' fees and costs) arising from or in any way related to Customer's use of the Location-Based Services application or information obtained in connection therewith.

AGREED TO AND ACCEPTED:

<b>CUSTOMER:</b> Kankakee County Sheriff's Department By: <u>Michael D. Downey</u> Name: <u>Michael D. Downey</u> Title: <u>Chief of Corrections</u> Date: <u>3/25/13</u>	<b>PROVIDER:</b> Securus Technologies, Inc. By: <u>Robert Pickens</u> Name: <u>Robert Pickens</u> Title: <u>Chief Operating Officer</u> Date: <u>3-29-13</u>
--	---

## **THREADS™ COMMUNITY USE AGREEMENT**

### **DESCRIPTION:**

The THREADS™ application allows authorized law enforcement users to analyze corrections and communications data from multiple sources to generate targeted investigative leads. THREADS™ has three main components: data analysis, data review, and data import. In addition, THREADS™ offers an optional “community” feature, which allows law enforcement and member correctional facilities to access and analyze corrections communications data from other corrections facilities within the community and data imported by other community members.

Customer’s community use of THREADS™ is governed by and conditioned upon execution of the THREADS™ Use Agreement. The obligations set forth therein are in addition to and not in lieu of the terms and conditions in the Agreement. In the event of a conflict between the Agreement and the terms of the THREADS™ Use Agreement, however, the THREADS™ Use Agreement shall prevail.

### **NATIONWIDE COMMUNITY FEATURE:**

Customer has elected to opt in to the community feature. The community feature allows authorized users access to analyze communications data generated from other corrections facilities within the community, as well as any data imported or added by other authorized community members. Customer acknowledges and understands that data from its facility or facilities will be made available to the community for analysis and review.

This THREADS™ Use Agreement is by and between [REDACTED] (“Customer”) and Securus Technologies, Inc., (“we,” “us,” or “Provider”) and is part of and governed by the Master Services Agreement (the “Agreement”) executed by the parties. The obligations set forth herein are in addition to and not in lieu of the terms and conditions of the Agreement, which are incorporated herein by reference. This THREADS™ Use Agreement shall be effective as of the last date signed by either party and shall be coterminous with the Agreement.

**1. COMPLIANCE WITH APPLICABLE LAWS.** Customer will comply with all privacy, consumer protection, marketing, and data security laws and government guidelines applicable to Customer’s access to and use of information obtained in connection with or through the THREADS™ application. Customer acknowledges and understands that the Customer is solely responsible for its compliance with such laws and that Provider makes no representation or warranty as to the legality of the use of the THREADS™ application or the information obtained in connection therewith. Provider shall have no obligation, responsibility, or liability for Customer’s compliance with any and all laws, regulations, policies, rules or other requirements applicable to Customer by virtue of its use of the THREADS™ application.

**2. SECURITY.** Customer acknowledges that the information available through the THREADS™ application includes personally identifiable information and that it is Customer’s obligation to keep all such accessed information secure. Accordingly, Customer shall (a) restrict access to THREADS™ to those law enforcement personnel who have a need to know as part of their official duties; (b) ensure that its employees (i) obtain and/or use information from the THREADS™ application only for lawful purposes and (ii) transmit or disclose any such information only as permitted or required by law; (c) keep all user identification numbers confidential and prohibit the sharing of user identification numbers; (d) use commercially reasonable efforts to monitor and prevent against unauthorized access to or use of the THREADS™ application and any information derived therefrom (whether in electronic form or hard copy); (e) notify Provider promptly of any such unauthorized access or use that Customer discovers or otherwise becomes aware of; and (f) unless required by law, purge all information obtained through the THREADS™ application and stored electronically or on hard copy by Customer within ninety (90) days of initial receipt or upon expiration of retention period required by law.

**3. PERFORMANCE.** Customer understands and acknowledges that all information used and obtained in connection with the THREADS™ application is “AS IS.” Customer further understands and acknowledges that

THREADS™ uses data from third-party sources, which may or may not be thorough and/or accurate, and that Customer shall not rely on Provider for the accuracy or completeness of information obtained through the THREADS™ application. Customer understands and acknowledges that Customer may be restricted from accessing certain aspects of the THREADS™ application which may be otherwise available. Provider reserves the right to modify, enhance, or discontinue any of the features that are currently part of the THREADS™ application. Moreover, if Provider determines in its sole discretion that the THREADS™ application and/or Customer's use thereof (1) violates the terms and conditions set forth herein and/or in the Agreement or (2) violates any law or regulation or (3) is reasonably likely to be so determined, Provider may, upon written notice, immediately terminate Customer's access to the THREADS™ application and shall have no further liability or responsibility to Customer with respect thereto.

**4. WARRANTIES/LIMITATION OF LIABILITY.** Provider shall have no liability to Customer (or to any person to whom Customer may have provided data from the THREADS™ application) for any loss or injury arising out of or in connection with the THREADS application or Customer's use thereof. If, notwithstanding the foregoing, liability can be imposed on Provider, Customer agrees that Provider's aggregate liability for any and all losses or injuries arising out of any act or omission of Provider in connection with the THREADS™ application, regardless of the cause of the loss or injury, and regardless of the nature of the legal or equitable right claimed to have been violated, shall never exceed \$100.00. Customer covenants and promises that it will not seek to recover from Provider an amount greater than such sum even if Customer was advised of the possibility of such damages. PROVIDER DOES NOT MAKE AND HEREBY DISCLAIMS ANY WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO THE THREADS™ APPLICATION. PROVIDER DOES NOT GUARANTEE OR WARRANT THE CORRECTNESS, COMPLETENESS, LEGALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OF THE THREADS™ APPLICATION OR INFORMATION OBTAINED IN CONNECTION THEREWITH. IN NO EVENT SHALL PROVIDER BE LIABLE FOR ANY INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, HOWEVER ARISING, INCURRED BY CUSTOMER FROM RECEIPT OR USE OF INFORMATION OBTAINED IN CONNECTION WITH THE THREADS™ APPLICATION OR THE UNAVAILABILITY THEREOF.

**5. INDEMNIFICATION.** Customer hereby agrees to protect, indemnify, defend, and hold harmless Provider from and against any and all costs, claims, demands, damages, losses, and liabilities (including attorneys' fees and costs) arising from or in any way related to Customer's use of the THREADS™ application or information obtained in connection therewith.

AGREED TO AND ACCEPTED:

CUSTOMER: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_